# Smart Grid Interoperability Panel - Cyber Security Working Group Standards Review

*Phase 2 Report*

**November 2, 2010**

# Security Assessment of Smart Meter Upgradeability

## 1. Introduction

### 1.1 Correlation of Cybersecurity with Information Exchange Standards

Correlating cybersecurity with specific information exchange standards, including functional requirements standards, object modeling standards, and communication standards, is very complex. There is rarely a one-to-one correlation, with more often a one-to-many or many-to-one correspondence.

Regardless of what information exchange standards are used, cybersecurity must be addressed from end-to-end. Cybersecurity must address procedures rather than technologies, such as authenticating the users and software applications, and screening personnel. Cybersecurity must also address how to: cope during an attack, recover from it afterwards, and create a trail of forensic information to be used in post-attack analysis. The cybersecurity requirements must reflect the environment where a standard is implemented rather than the standard itself; how and where a standard is used must establish the levels and types of cybersecurity needed.

Some standards do not mandate their provisions using "shall" statements, but rather use statements such as "should," "may," or "could." Some standards also define their provisions as being "normative" or "informative." Normative provisions often are expressed with "shall" statements. Various standards organizations use different terms (e.g., standard, guideline) to characterize their standards according to the kinds of statements used. If standards include security provisions, they need to be understood in the context of the "shall," "should," "may," and/or "could" statements, "normative," or "informative" language with which they are expressed.

Therefore, cybersecurity must be viewed as a stack or "profile" of different security technologies and procedures, woven together to meet the security requirements of a particular implementation of a stack of policy, procedural, and communication standards designed to provide specific services. Ultimately, cybersecurity as applied to the information exchange standards should be described as profiles of technologies and procedures which can include both "power system" methods (e.g. redundant equipment, analysis of power system data, and validation of power system states) and information technology (IT) methods (e.g. encryption, role-based access control, and intrusion detection).

In the following discussion, these caveats should be taken into account.

### 1.2 Standardization Cycles of Information Exchange Standards

Functional and communication standards, regardless of the standards organization, are developed over a time period of many months by experts who are trying to meet a specific need. In most cases, these experts are expected to revisit standards every five years in order to determine if updates are needed. In particular, since cybersecurity requirements were often not included in standards in the past, existing communication standards often have no references to security except in generalities, using language such as "appropriate security technologies and procedures should be implemented."

Since technologies (including cybersecurity technologies) are rapidly changing to meet increasing new and more powerful threats, some cybersecurity standards can be out-of-date by the time they are released. This means that some requirements in a security standard may be inadequate (due to new technology developments), while references to other security standards may be obsolete. This rapid improving of technologies and obsolescence of older technologies is impossible to avoid, but may be ameliorated by indicating minimum requirements and urging fuller compliance to new technologies as these are proven.

### 1.3 References and Terminology

References to the National Institute of Standards and Technology (NIST) security requirements refer to the NIST Interagency Report (IR) 7628, *Guidelines to Smart Grid Cyber Security*, Chapter 3, High-Level Security Requirements.

References to "government-approved cryptography" refer to the list of approved cryptography suites identified in Chapter 4, Cryptography and Key Management, of NISTIR 7628. Summary tables of the approved cryptography suites are provided in Chapter 4.3.2.1.

As noted, standards have different degrees for expressing requirements, and the security requirements must match these degrees. For these standards assessments, the following terminology is used to express these different degrees[1]:

- Requirements are expressed by "…shall…," which indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).
- Recommendations are expressed by "…should…," which indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).
- Permitted or allowed items are expressed by "…may…," which is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).
- Ability to carry out an action is expressed by "…can …," which is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).
- The use of the word *must* is deprecated, and should not be used in these standards to define mandatory requirements. The word *must* is only used to describe unavoidable situations (e.g. "All traffic in this lane must turn right at the next intersection.")

## 2. NEMA SG-AMI 1-2009: Requirements for Smart Meter Upgradeability

### 2.1 Description of Standard

NEMA SG-AMI 1 (also known as the Smart Meter Upgradeability standard) is a set of functional requirements for Smart Meter firmware upgradeability in the context of an Advanced Metering Infrastructure (AMI) system for industry stakeholders such as regulators, utilities, and vendors. The NIST Smart Grid Interoperability Panel (SGIP) Priority Action Plan (PAP) 00, Meter Upgradeability Standard, completed this standard in September 2009.

Specifically, "*The following serves as a key set of requirements for Smart Meter upgradeability. These requirements should be used by Smart Meter suppliers, utility customers, and key constituents, such as regulators, to guide both development and decision making as related to Smart Meter upgradeability. The purpose of this document is to define requirements for Smart Meter Firmware upgradeability in the context of an AMI system for industry stakeholders such as regulators, utilities, and vendors. NEMA Smart Grid Standards Publication SG-AMI 1 defines requirements that include secure local and remote upgrades of Smart Meter:*

- *Metrology;*

[1] The first clause of each terminology definition comes from the International Electrotechnical Commission (IEC) Annex H of Part 2 of ISO/IEC Directives. The second clause (after "which") comes from the Institute of Electrical and Electronics Engineers (IEEE) as a further amplification of the term.

- *AMI applications;*
- *AMI communications;*
- *HAN applications; and*
- *HAN communications.*

*Upgrading of devices other than Smart Meters is beyond the scope of this document.*[2]"

The standard includes five sections:

1. General
2. Definitions
3. Upgrade Process Functional Requirements
4. Upgrade Process Security Requirements
5. Reference Diagram

## 2.2 Assumptions

Since this standard addresses only one aspect of metering, its security requirements are (and should be) limited only to that aspect and should not be expected to address the overall metering security requirements. For this reason, security policies and other "common" security governance requirements are not expected to be included in this standard: only security requirements related to upgradeability are covered in this assessment. Any recommendations for changes within this document will use this assumption.

This standard defines functional requirements only. Functional requirements describe "what" is needed, but not "how" to implement or which specific technologies to use. Therefore, the cybersecurity issues are assessed on how well they address "what" security is needed, not on "how" these security requirements are to be met.

In addition, these NEMA functional requirements are at such a high level that many of the NISTIR 7628 security requirements are addressed by each of these functional requirements.

This standard does cover "requirements," and thus uses the term "shall" for those requirements.

## 2.3 Summary of Cybersecurity Content

### 2.3.1 Does the standard address cybersecurity? If not, should it?

NEMA SG-AMI consists of two sections of requirements: the Upgrade Process Functional Requirements and the Upgrade Process Security Requirements.

In Section 3, Upgrade Process Functional Requirements, the Smart Meter subsection covers general security requirements for logging, integrity, trusted sourcing, and authorization. The Metrology, AMI Applications and Communications, and HAN Applications and Communications subsections do not specifically reference any additional security requirements, while the Upgrade Management System subsection refers to the Upgrade Process Security Requirements section.

In Section 4, Upgrade Process Security Requirements, the document covers the following specific requirements for cybersecurity for upgradeability:

- Cryptography
- Compromise

[2] NEMA Smart Grid Standards Publication SG-AMI 1-2009: *Requirements for Smart Meter Upgradeability*

- Authentication
- Integrity of commands
- Privacy
- Forgery
- Defense in depth
- Intrusion / anomaly detection
- Logging
- Auditing

### 2.3.2 What aspects of cybersecurity does the standard address and how well (correctly) does it do so?

Functional requirements describe "what" is necessary, but not "how" to implement or which specific technologies to use. Therefore, the cybersecurity issues addressed by the Meter Upgradeability Functional Requirements Standard were assessed on how well they address "what" security is needed, rather than "how" these security requirements are to be met.

In this standard, the functional security requirements map to the requirements within NISTIR 7628, including:

- Access control,
- Audit and accountability,
- Authorization,
- Identification and authentication,
- System development and maintenance,
- Information system and communication protection, and
- Information integrity.

It also mentions specific encryption suites.

The correlations between this standard and the security requirements described in NISTIR 7628, *Guidelines to Smart Grid Cybersecurity*, Chapter 3, families and requirements, are shown in Table 1:

**Table 1: Correlations between Standard being Assessed and the NISTIR Security Requirements**

| Reference in Standard[3] | Applicable NISTIR 7628 Requirement | Comments if NISTIR Requirement Is Not Completely Met |
|---|---|---|
| **3.2 Smart Meter** | | |
| 3.2.1 | SG.CM-8, Component Inventory | |
| | SG.IA-5, Device Identification and Authentication | |
| | SG.MA-3, Smart Grid Information System Maintenance | |
| 3.2.2 | SG.CP-10, Smart Grid Information System Recovery and Reconstitution | |

[3] The references may be just the section numbers or could include the title of the section

| Reference in Standard[3] | Applicable NISTIR 7628 Requirement | Comments if NISTIR Requirement Is Not Completely Met |
|---|---|---|
| | SG.CP-11, Fail-Safe Response | |
| | SG.CP-2 Continuity of Operations Plan | |
| | SG.SC-22, Fail in Known State | |
| 3.2.3 | SG.CM-3, Configuration Change Control | |
| | SG.SC-8, Communication Integrity | |
| 3.2.4 | SG.SC-8, Communication Integrity | |
| | SG.SI-7, Software and Information Integrity | |
| | SG.SI-8, Information Input Validation | |
| 3.2.5 | SG.AU-1, Audit and Accountability | |
| | SG.AU-2, Auditable Events | |
| | SG.CM-4, Monitoring Configuration Changes | |
| 3.2.7 | SG.CM-3, Configuration Change Control | |
| | SG.CM-6, Configuration Settings | |
| 3.2.9 | SG.CA-5, Security Authorization to Operate | |
| | SG.CM-3, Configuration Change Control | |
| 3.2.10 | SG.CM-3, Configuration Change Control | |
| | SG.CM-5, Access Restrictions for Configuration Change | |
| | SG.IA-4, User Identification and Authentication | |
| | SG.IA-5, Device Identification and Authentication | |
| | SG.SC-20, Message Authenticity | |
| 3.2.11 | SG.SA-11, Supply Chain Protection | |
| | SG.SC-10, Trusted Path | |
| | SG.SC-21, Secure Name/Address Resolution Service | |
| **3.3 Metrology** | | |
| 3.3.1 | SG.CM-3, Configuration Change Control | |
| | SG.CM-6, Configuration Settings | |
| **3.4 AMI Applications and Communications** | | |
| 3.4.1 | SG.CM-3, Configuration Change Control | |
| | SG.CM-6, Configuration Settings | |

| Reference in Standard[3] | Applicable NISTIR 7628 Requirement | Comments if NISTIR Requirement Is Not Completely Met |
|---|---|---|
| **3.5 HAN Applications and Communications** | | |
| 3.5.1 | SG.CM-3, Configuration Change Control | |
| | SG.CM-6, Configuration Settings | |
| **3.6 Upgrade Management System** | | |
| 3.6.1 | SG.CM-3, Configuration Change Control | |
| | SG.CM-6, Configuration Settings | |
| 3.6.2 | SG.CP-10, Smart Grid Information System Recovery and Reconstitution | |
| **4. Upgrade Process Security Requirements** | | |
| 4.1 | SG.SC-12, Use of Validated Cryptography | |
| | SG.SC-14, Transmission of Security Parameters | |
| 4.2 | SG.SC-11, Cryptographic Key Establishment and Management | |
| 4.3 | SG.SC-5 Denial-of-Service Protection | |
| | SG.SC-7 Boundary Protection | |
| | SG.SI-6, Security Functionality Verification | |
| 4.4 | SG.AC-4, Access Enforcement | The requirements in the Smart Meter Upgradeability standard are addressed at a very high level with little specific detail. |
| | SG.AC-12, Device Identification and Authentication | |
| | SG.AC-15, Remote Access | |
| | SG.SC-8, Communication Integrity | |
| | SG.SC-20, Message Authenticity | |
| 4.5 | SG.AC-7, Least Privilege | |
| | SG.CA-5, Security Authorization to Operate | |
| | SG.CM-5, Access Restrictions for Configuration Change | |
| 4.6 | SG.CP-2 Continuity of Operations Plan | |
| | SG.PL-4, Privacy Impact Assessment | |
| 4.7 | SG.AU-16, Non-Repudiation | |
| | SG.SC-8, Communication Integrity | |
| | SG.SC-20, Message Authenticity | |
| | SG.SI-7, Software and Information Integrity | |
| 4.8 | SG.SC-7, Boundary Protection | |
| 4.9 | SG.AU-2, Auditable Events | |

| Reference in Standard[3] | Applicable NISTIR 7628 Requirement | Comments if NISTIR Requirement Is Not Completely Met |
|---|---|---|
| | SG.CM-6, Configuration Settings | |
| | SG.IR-5, Incident Handling | |
| | SG.IR-6, Incident Monitoring | |
| | SG.SC-8, Communication Integrity | |
| | SG.SI-4, Smart Grid Information System Monitoring Tools and Techniques | |
| 4.10 | SG.AU- 2, Auditable Events | |
| | SG.AU-6 Audit Monitoring, Analysis, and Reporting | |
| | SG.IR-7 Incident Reporting | |

### 2.3.3 What aspects of cybersecurity does the standard not address? Which of these aspects should it address? Which should be handled by other means?

NEMA SG-AMI 1 covers most aspects of cybersecurity that are relevant to meter upgradeability. It is expected that other AMI-related standards do, will, or should address more general AMI and metering security requirements, such as account management, security training, strategic planning, risk management, and cryptographic key management. It is expected that these AMI security requirements will be identified by the CSWG in the AMI Security Subgroup. Therefore, it is acceptable that this standard not address the more general cybersecurity requirements for meters and AMI systems.

However, it is recommended that a few additional cybersecurity requirements that are directly pertinent to meter upgrading should be covered within this standard. These include:

- Physical access and environmental security for upgrades handled by local access methods.
- Maintenance of a secure, intact audit log (i.e., not modified or erased) during upgrade, that logs the upgrade process as well as any other events that occur during the upgrade.
- Protection of timestamps and time synchronization during upgrades.

### 2.3.4 What work, if any, is being done currently or planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

Currently NEMA SG-AMI 1-2009 does not have a time frame for enhancing the standard, but it is expected that those responsible would be open to receiving comments.

### 2.3.5 List any references to other standards and whether they are normative or informative.

There are no normative or informative references within the standard.